JOURNAL OF ALGEBRA 96, 94–113 (1985)

Subgroups Inducing the Same Permutation Representation, II

ROBERT M. GURALNICK

Department of Mathematics, University of Southern California, Los Angeles, California 90089

AND

DAVID B. WALES

Department of Mathematics, California Institute of Technology, Pasadena, California 91125

Communicated by Walter Feit

Received March 12, 1984

1. INTRODUCTION

Let R be a principal ideal domain and G a finite group. Denote by I_G the RG-module which is isomorphic to R as an R-module and has trivial action by G. If H is a subgroup of G, let $(I_H)^G = RG \otimes_{RH} I_H$ denote the induced module. This is a free R-module with a basis which is a G-orbit such that H is the stabilizer of some element in the basis. The problem considered in this article is to determine when G contains nonconjugate subgroups H and K such that $(I_H)^G \cong (I_K)^G$ as RG-modules. This has been considered for a field of characteristic zero in [13]. Our first result gives a criterion for this to hold when $R = \mathbb{Z}_p$, the ring of p-adic integers and $|G:H| = p^a$.

THEOREM A. *Let R be a (complete) discrete valuation ring with residue field of characteristic p. Let $P \in \mathrm{Syl}_p(G)$ and let H and K be subgroups of index p^a in G. The following are equivalent*:

(a) $(I_H)^G \cong (I_K)^G$ *as RG-modules.*

(b) $P \cap H$ *and* $P \cap K$ *are conjugate in G.*

A more general result is proved in Section 2. The result is closely related to Scott modules (see Burry [3] and Green [12]). Also, if $P \cap H = e$, I_H^G is the principal indecomposable and Theorem A follows from its properties

0021-8693/85 $3.00

[2, 15]. In that case the first author [13] has shown using the classification of simple groups that unless $p^b = (q^n - 1)/(q-1)$ for some b, $n \geqslant 3$, and prime power q, H and K must be conjugate.

Besides the intrinsic interest in studying isomorphism of permutation modules, there are number theoretic consequences. Let E and F be number fields (i.e., finite extensions of the rational numbers $\mathbb{Q}$). Perlis [18] showed that E and F have the same zeta function if and only if they have the same normal closure D and $(I_H)^G \cong (I_K)^G$ (over $\mathbb{Q}$) where H and K are the subgroups of $G = Gal(D/\mathbb{Q})$ corresponding to E and F. Such fields are called arithmetically equivalent. Clearly, $E \cong F$ if and only if H and K are conjugate. Moreover, if $(I_H)^G \cong (I_K)^G$ over $\mathbb{Z}_p$, then $h(E)_p \cong h(F)_p$ where $h(E)_p$ denotes the Sylow p-subgroup of the class group of E. Hence an immediate consequence of Theorem A is:

COROLLARY 1. *Let E and F be extensions of $\mathbb{Q}$ of degree p^a with the same normal closure D. If there exists $\sigma \in \mathrm{Aut}(D)$ such that $p^{a+1} \nmid [E\sigma(F) : \mathbb{Q}]$ then*

(a) *E and F are arithmetically equivalent, and*

(b) *$h(E)_p \cong h(F)_p$.*

Perlis [19] obtained the corollary in case $a = 1$. Note in this case that $p^2 \nmid [EF : \mathbb{Q}]$ since $p^2 \nmid [D : \mathbb{Q}]$.

We also consider the relationship of permutation modules when the ring is changed. Clearly p-adic isomorphism implies both rational isomorphism and isomorphism over fields of characteristic p. Surprisingly, isomorphism over fields of characteristic p implies p-adic isomorphism (Theorem 2.9). In general, rational isomorphism does not imply p-adic isomorphism. However, this is true for subgroups of index p or p^2 (Corollary 4.2). By [13], if n is divisible by p^3 for some prime p, there exists a nilpotent group G with nonconjugate subgroups H and K of index n such that $(I_H)^G \cong (I_K)^G$ (over $\mathbb{Q}G$).

A next case to consider is $n = pq$. In Section 5, we determine some general facts about subgroups of squarefree index. In Section 6, we essentially describe all permutation groups of degree pq and as a consequence prove:

THEOREM B. *Let p and q be distinct primes. Suppose $[G : H] = pq$ and $(I_H)^G \cong (I_K)^G$ (as $\mathbb{Q}G$-modules). One of the following holds:*

(a) *H and K are conjugate.*

(b) *p, q, or $pq \in \Omega = \{r \mid r = (l^n - 1)/(l-1)$, l a prime power, $n \geqslant 3$ or $r = 11\}$.*

(c) *q is a Fermat prime and* $q \equiv 2 \bmod p$ (*or vice versa*).

(d) $pq = 29 \cdot 59$.

Moreover, for (b)–(d), *there exist G, H, K satisfying the hypotheses with H and K nonconjugate.*

Theorem B depends on the classification of simple groups. However, one case worth noting is independent of that; namely, if G is solvable, then H and K are conjugate (Theorem 6.1).

In Section 3, we give some examples of nonconjugate subgroups inducing the same permutation representation. Combining the examples and the theorems shows that for $18 \neq n \leqslant 40$, there exist examples with nonconjugate subgroups of index n inducing the same permutation character if and only if $n \geqslant 7$ and $n \neq 9$, 10, 17, 19, 23, 25, 29, 37, or 38. The case $n = 18$ is still open. There is a related result for arithmetically equivalent fields of degree n assuming the groups do occur as Galois groups.

Notation is as in [13].

2. p-ADIC ISOMORPHISM

Assume in this section (unless stated otherwise) that R is a complete discrete valuation ring with residue field $\bar{R}$ of characteristic p. In particular, one can take R to be $\mathbb{Z}_p$, the p-adic integers, or a field of characteristic p. Let G be a finite group with subgroups H and K of index n. Let $V = I_H^G$ and $W = I_K^G$ be the (left) RG-modules induced by the action of G on the left cosets of H and K, respectively. The main results of this section are Theorem 2.1, its Corollary, and Theorem 2.9.

THEOREM 2.1. *If $V \cong W$, then the Sylow p-subgroups of H and K are conjugate. Conversely, if the Sylow p-subgroups of H and K are conjugate and V is indecomposable, then $V \cong W$ (as RG modules).*

COROLLARY 2.2. *If $n = p^a$, then $V \cong W$ if and only if the Sylow p-subgroups of H and K are conjugate.*

These results can also be obtained by using properties of Scott modules and properties of vertices and sources and are inherent in [3] and [12] when R is a field. We present a proof of these results without using these concepts and discuss the relationship with them. The proof follows from a series of lemmas.

The first result is the Mackey Decomposition Theorem and holds for any commutative ring. See [9] for a proof and note (ii) is a special case of (i).

LEMMA 2.3. (i) *If* $M \leqslant G$, *then* $(I_H^G)_M \cong \bigoplus_{x \in \Delta} I^M_{M \cap H^x}$, *where* Δ *is a set of* (M, H) *double coset representatives.*

(ii) *If* $I_H^G \cong I_K^G$ *and* $G = HM$, *then* $G = KM$ *and* $I^M_{M \cap H} \cong I^M_{M \cap K}$.

LEMMA 2.4. *If* $n = [G : H] = p^a$, *then* V *is indecomposable.*

Proof. Let P be a Sylow p-subgroup of G. Then $G = PH$. By the previous lemma, $V_P \cong I^P_{P \cap H}$. Set $\bar{V} = V \otimes_R \bar{R}$. If V is decomposable, then so is $\bar{V}$. As P acts transitively on the cosets of $P \cap H$, P fixes a unique line in $\bar{V}$. Since P fixes a line in each summand of $\bar{V}$, it follows that $\bar{V}_P$ is indecomposable and so $\bar{V}$ as well. This means V is indecomposable.

LEMMA 2.5. *If* $V \cong W$, $Q \in \mathrm{Syl}_p(H)$ *and* $R \in \mathrm{Syl}_p(K)$, *then* Q *and* R *are conjugate in* G.

Proof. By Lemma 2.3,

$$V_Q \cong \bigoplus_{x \in \Delta} I^Q_{Q \cap H^x} \cong \bigoplus_{x \in \Delta'} I^Q_{Q \cap K^x} \cong W_Q$$

where Δ and Δ' are sets of representatives for the (Q, H) and (Q, K) double cosets. Since each of the summands is indecomposable, it follows by the Krull Schmidt Theorem (which holds for RG, see [9, Vol. II, 43.7]) that $I^Q_{Q \cap H} = I^Q_Q \cong I^Q_{Q \cap K^x}$ for some x.

Thus $I^Q_{Q \cap K^x}$ is one dimensional and $K^x \geqslant Q$. Now Q and R^x are both Sylow p-subgroups of K^x, and Q and R are conjugate by Sylow's Theorem.

LEMMA 2.6. *Let* $Q \in \mathrm{Syl}_p(H)$. *Then* V *is a direct summand of* $U = I_Q^G$ *(as* RG*-modules).*

Proof. Let $\{u_1, ..., u_s\}$ be an R basis for U such that Q fixes u_1 and G permutes the u_i. Similarly, choose $\{v_1, ..., v_n\}$ a basis for V such that $Hv_1 = v_1$ and G permutes the v_i. Let $x_1, ..., x_m$ be left coset representatives for Q in H. Define α: $V \to U$ and β: $U \to V$ by

$$\alpha g v_1 = \frac{1}{m} \sum_{i=1}^{m} g x_i u_1,$$

and

$$\beta g u_1 = g v_1.$$

Note α and β are well defined RG homomorphisms and $\beta\alpha$ is the identity $(p \nmid m$, so $m^{-1} \in R)$. Thus α is injective, and so $U \cong V \oplus \mathrm{Ker}\, \beta$.

LEMMA 2.7. *If H and K have conjugate Sylow p-subgroups and V is indecomposable, then $V \cong W$.*

Proof. By conjugation assume Q is a Sylow p-subgroup of both H and K. By Lemma 2.6, V and W are both summands of $I_Q^G = U$. Write $U = \oplus U_i$, where each U_i is indecomposable. By the Krull Schmidt Theorem, $V \cong U_i$ for some i and $W \cong \oplus U_j$, $j \in J$, for some subset J. Since U is a permutation module, there is a unique line in U on which G acts trivially. Thus exactly one U_j has such a submodule. Since V contains a trivial submodule, it must be $U_i \cong V$. As W has such a submodule, $i \in J = \{i\}$ since V and W are free rank n R-modules.

Theorem 2.1 now follows from Lemmas 2.3 through 2.7 and Corollary 2.2 follows from the theorem and Lemma 2.4.

Remarks. (1) If H is a p-complement, I_H^G is the principal p-indecomposable and these results follow from its properties [2, 15].

(2) These results can be proved using the theory of Scott modules, vertices, and sources. As in Lemma 2.7, any transitive permutation module U has a unique indecomposable constituent containing a trivial submodule. This is called the Scott module of U. Denote this by $S(U)$. This is precisely the definition of Scott module given in [3] or [12] if R is a field of characteristic p. The same definition applies equally well if R is a complete discrete valuation ring. Some properties will apply over a general such ring, but others will not. Arguments as in the proofs of the lemmas show that $S(V)$ has vertex Q for any $Q \in \mathrm{Syl}_p(H)$. Hence $V \cong W$ implies that $S(V) \cong S(W)$ have the same vertex yielding the first part of the theorem. If V is indecomposable, then $V = S(V)$ and one can argue as in Lemma 2.7. (See Burry [3] or Green [12] for the case R is a field.) With this terminology, the proof of Lemma 2.7 provides a proof of Lemma 2.7′.

LEMMA 2.7′. *If $V = I_H^G$ and $W = I_K^G$, then $S(V) \cong S(W)$ if and only if H and K have conjugate Sylow p-subgroups.*

(3) Theorem 2.1 and Corollary 2.2 remain valid if I_H^G is replaced by any linear character λ of G (that is, take $V = \lambda_H^G$ and $W = \lambda_K^G$). The proof is as given with the obvious modifications.

We show below that the decomposition into indecomposables of a permutation module over R has a special property not enjoyed by RG-modules in general. To be specific, let V be a permutation module and let $V = V_1 \oplus \cdots \oplus V_r$ be the decomposition into indecomposable submodules. Then $\bar{V} = \bar{V}_1 \oplus \cdots \oplus \bar{V}_r$ is the decomposition into *indecomposable* $\bar{R}G$-submodules. Thus V_i is indecomposable if and only if $\bar{V}_i$ is indecomposable. This is not necessarily true for R-modules in general although if $\pi^e \nmid |G|$, then $V/\pi^e V \cong W/\pi^e W$ implies $V \cong W$ where π is the maximal ideal of R

[17]. This helps explain why the statement of Theorem 2.1 is the same using either R or $\bar{R}$ (assuming the indecomposability of the module).

LEMMA 2.8. $\dim_R \mathrm{Hom}_{RG}(V, W) = \dim_{\bar{R}} \mathrm{Hom}_{\bar{R}G}(\bar{V}, \bar{W})$.

Proof. By Frobenius reciprocity [9, 11], $\mathrm{Hom}_{RG}(V, W)$ is R-isomorphic to $\mathrm{Hom}_{RH}(I_H, (I_K^G)_H)$. This latter module is clearly R-isomorphic to $C_W(H)$, the fixed space of H on W. Moreover, $C_W(H)$ is a free rank d R-module, where d is the number of orbits of H on the cosets of K. By replacing R by $\bar{R}$ in the argument above, we see both dimensions are d.

THEOREM 2.9. (i) $\bar{V} \cong \bar{W} \Leftrightarrow V \cong W$.

(ii) *If $V = \bigoplus V_i$, where each V_i is indecomposable, then $\bar{V}_i$ is indecomposable. In particular, V is indecomposable if and only if $\bar{V}$ is. Also, if $S(V)$ and $S(\bar{V})$ are the Scott modules of V and $\bar{V}$, respectively, then $S(\bar{V}) = \overline{S(V)}$.*

Proof. Let (π) be the maximal ideal of R. Suppose $\bar{V} \cong \bar{W}$. By choosing bases for V and W, any element α in $\mathrm{Hom}_{RG}(V, W) = B$ can be represented by an $n \times n$ matrix. The map φ sending $\alpha \to \bar{\alpha}$ in $\mathrm{Hom}_{\bar{R}G}(\bar{V}, \bar{W}) = \bar{B}$ given by reduction $\bmod \pi$ is an R homomorphism. Moreover, $\dim_R B = \dim_{\bar{R}} \varphi(B)$. By the previous result, this implies $\varphi(B) = \bar{B}$. Since $\bar{V} \cong \bar{W}$, there exists an isomorphism γ in C. Thus $\gamma = \varphi(\alpha)$ for some α in B. Considering α as a matrix, we see $\det \alpha \notin (\pi)$ as $\det(\gamma) \neq 0$. Thus $\det \alpha$ is a unit and α is an isomorphism. (Alternatively, one can give a coordinate free proof using Nakayama's Lemma.)

The argument above shows that any homomorphism from $\bar{V}$ to $\bar{W}$ comes from an element of $\mathrm{Hom}_{RG}(V, W)$. In particular, this holds for $W = V$. So assume, say, $\bar{V}_1$ is decomposable. Thus there exists an idempotent $\gamma \neq 0$ or 1 in $\mathrm{End}_{RG}(\bar{V}_1)$. By the above remarks, there is some $\alpha \in \mathrm{End}_{RG}(V_1) = E$ inducing γ on $\bar{V}_1$. Hence $\alpha^2 - \alpha \in \pi E$.

Since R is complete, there exists $\beta \in E$ with $\beta^2 = \beta$ and $\beta - \alpha \in \pi E$. In particular, $\beta \neq 0$ or 1 in E. Thus $V_1 = \beta(V_1) \oplus \ker \beta$. This contradicts the indecomposability of V_1 and proves the result.

That $\overline{S(V)} = S(\bar{V})$ follows because $\overline{S(V)}$ is indecomposable and has a trivial submodule.

We now discuss a method for showing in certain situations that I_H^G is indecomposable as an RG-module. Let $P \in \mathrm{Syl}_p(G)$ and $P \geqslant Q \in \mathrm{Syl}_p(H)$. Assume also that R has characteristic zero and K is its quotient field. If $V = V_1 \oplus V_2$ decomposes, then $V \otimes_R K = (V_1 \otimes_R K) \oplus (V_2 \otimes_R K)$. Hence the permutation character of $V \otimes_R K$ is $\chi_1 + \chi_2 + \cdots + \chi_t$ where $\chi_1 = 1$ and for $i > 1$, the χ_i are nontrivial characters. Hence

$$\dim V_i = \sum_{j \in J_i} \chi_j(1)$$

where J_1 and J_2 are a partition of $\{1, ..., t\}$. Moreover, by Lemmas 2.3 and 2.4, $[P:Q] \mid \dim V_i$. In particular, if the permutation representation is doubly transitive, then V is indecomposable if and only if $p \nmid [G:H]$. Similarly, if the permutation representation is rank three, then the character is of the form $1 + \chi_2 + \chi_3$, and if $p^a \mid [G:H]$ and $p^a \nmid \chi_2(1)$ or $\chi_3(1)$, then V is indecomposable.

We close this section with a related result which we shall require later. This result holds for an arbitrary commutative ring.

LEMMA 2.10. *If $A \lhd G$ and $I_H^G \cong I_K^G$, then $I_{HA}^G \cong I_{KA}^G$.*

Proof. Again, let $V = I_H^G$. We shall show $U = C_V(A) \cong I_{HA}^G$ which thus must be isomorphic to I_{KA}^G.

Choose an R basis $B = \{v_{ij}\}$ for V such that B is a G orbit, H fixes v_{11}, and $O_j = \{v_{1j}, ..., v_{sj}\}$ is an A orbit for each j. Set $u_j = v_{1j} + \cdots + v_{sj}$. As $A \lhd G$, G permutes the O_j and so the $\{u_j\}$. Indeed since G is transitive, $\{u_j\}$ is a G orbit. Clearly U is the R span of the $\{u_j\}$, and so $\{u_j\}$ is a basis for U. Since $Hu_{11} = v_{11}$, $gu_1 = u_1 \Leftrightarrow gO_1 = O_1 \Leftrightarrow g \in HA$. Therefore $U \cong I_{HA}^G$.

3. EXAMPLES

In this section we present several examples which apply to Section 2 and later sections.

EXAMPLE 1: Higman–Sims Group [14]. The Higman–Sims Group has two conjugary classes of subgroups of index 176 which are permuted by an outer automorphism. The action on the cosets of each is doubly transitive. Each subgroup is isomorphic to $P\Gamma U(3, 5)$. Note here $176 = 11 \cdot 16$.

First let R be the 11-adic integers. Let H be a representative of one of the conjugate classes of $P\Gamma U(3, 5)$ subgroups and K a representative of the other. As the representations are both doubly transitive, V is indecomposable. As H and K have the same Sylow 11-subgroup, $I_H^G \cong I_K^G$ over R. This means they are also isomorphic over $\mathbb{C}$ and over $\bar{R}$.

Next let R be the 2-adic integers. Then K acts on the cosets of H in two orbits of sizes 126 and 50. As these are even, a Sylow 2-subgroup of K does not fix any point and so no Sylow 2-subgroup of K is contained in any conjugate of H. This shows that over R, the modules are not isomorphic by Theorem 2.1. If R is a finite field of characteristic 2, the module V is also indecomposable by Theorem 2.9. Again the modules are not isomorphic.

This is an example of permutation modules which are indecomposable over $GF(2)$ and $GF(11)$. They are isomorphic over $GF(11)$ and so over $\mathbb{C}$, but not over $GF(2)$.

EXAMPLE 2: M_{23}. As seen from Table I in Section 5, M_{23} has two permutation representations of degree 253. The stabilizers of points are not isomorphic subgroups; one being $M_{21}*2$ and the other 2^4A_7. The permutation characters are both the same with degrees 1, 22, 230. The orbits of the stabilizers of a point have different lengths; 1, 42, 210 for the $M_{21}*2$ and 1, 112, 140 for 2^4A_7. Note $253 = 23 \times 11$. They are decomposable over $GF(11)$ and $GF(23)$ as the character of degree 22 is an 11-projective and the character of degree 230 is a 23-projective. They are isomorphic over $\mathbb{C}$. This shows that two permutation representations isomorphic over $\mathbb{C}$ need not have isomorphic point stabilizers.

EXAMPLE 3. This is a general class of examples which provide several specific groups of interest. Suppose G is a group with an outer automorphism σ. Let H be a subgroup and suppose x^σ is conjugate to an element in $\langle x \rangle$ for each x in H. Then the permutation character on the cosets of H is the same (over $\mathbb{C}$) as the permutation character on the cosets of H^σ. This follows as in any permutation representation, the number of points fixed by x is the same as the number fixed by $\langle x \rangle$.

Suppose also that $Y \subseteq H \subseteq N(Y)$ with Y a Sylow p-subgroup of G. The notation $A \sim B$ in G for A, B subgroups of G means $g^{-1}Ag = B$ for some g in G. Now $H^\sigma \sim K$ in $N(Y)$ and $H \sim H^\sigma$ in G if and only if $H \sim K$ in $N(Y)$. To see this choose g in G such that $(Y^\sigma)^g = Y$. Then $K = H^{\sigma g} \subseteq N(Y)$. If $K = H^l$ for $l \in G$, $Y^{\sigma g} = Y$ is the Sylow p-group of H^l and so $Y^l = Y$ and $l \in N(Y)$. This means that if $H \sim K$ in G, $H \sim K$ in $N(Y)$.

A class of such groups can be obtained from $GL_n(q)$. Let $G = GL_n(q)$,

$$H = \left\{ \begin{pmatrix} d_1 & * & \cdots & * \\ & & \ddots & \vdots \\ 0 & & & * \end{pmatrix} ; d_1 \text{ is in a subgroup of index } s \text{ of } (GF(q))^* \right\}.$$

Let $\sigma\colon A \to (A^{-1})^t$ and

$$Y = \left\{ \begin{pmatrix} 1 & & & * \\ & 1 & & \\ & & 1 & \\ 0 & & & 1 \end{pmatrix} \right\}.$$

Then

$$\tau = \begin{pmatrix} 0 & & 1 \\ & \cdot^{\cdot^{\cdot}} & \\ 1 & & 0 \end{pmatrix}$$

conjugates H^σ to the subgroup

$$K=\left\{\begin{pmatrix} * & \cdots & * \\ & \ddots & \vdots \\ & & * \\ 0 & & d_1 \end{pmatrix}\right\}$$

of $N(Y)$. Unless $s=1$, K is not conjugate to H in

$$N(Y)=\left\{\begin{pmatrix} * & \cdots & * \\ & \ddots & \vdots \\ 0 & & * \end{pmatrix}\right\}$$

and so the permutation representation on the cosets of H and K are isomorphic over $\mathbb{C}$ but the stabilizers of the points are not conjugate. Note σ is the graph automorphism.

EXAMPLE 3a. Set $n=2$, $l=3$, $p=2$. The index in $GL_2(3)$ is $2\cdot(3^2-1)/(3-1)=8$. This gives two subgroups of $GL_2(3)$ of index 8 which are not conjugate but have the same permutation character over $\mathbb{C}$. Both subgroups have conjugate Sylow 2-subgroups; namely, $\left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \pm 1 \end{smallmatrix}\right)$. This means the modules are isomorphic over $\mathbb{Z}_2$ or a field of characteristic 2. Perlis [18] constructed an example of order 32 with the modules not isomorphic over $\mathbb{Z}_2$. Since $GL_2(3)$ is a Galois group over $\mathbb{Q}$ this gives examples of nonisomorphic fields with the same zeta function and whose class groups have isomorphic Sylow 2-subgroups.

EXAMPLE 3b. Set $n=2$, $q=2$, (2^l+1) a Fermat prime, and $p \mid 2^l-1$. This gives subgroups of index $p(2^l+1)$. For example if $l=2$, $GL_2(4)$ has two subgroups of index $5\cdot 3=15$. In later sections, we will consider subgroups of index pq where p and q are distinct primes. This example gives situations where such subgroups arise.

EXAMPLE 3c. Let $G=GL_n(r)$, M the stabilizer of a line, $n\geqslant 3$. Let σ again denote the graph automorphism on G (e.g., $\sigma(g)=(g^t)^{-1}$). Now $M/M'\cong Z_{r-1}\times Z_{r-1}$. Choose a subgroup H of M such that $M/H\cong Z_q$ (so $r\equiv 1 \bmod q$) and set $K=H^\sigma$. Then $I_H^G=I_K^G$, and $M=N_G(H)$ is not conjugate to M^σ (which is the stabilizer of a hyperplane). Thus H and K are not conjugate. In particular, choose H so that H does not contain $Z=Z(G)$. Thus if q is prime, $[Z:H\cap Z]=q$. Now let $\bar{G}=G/H\cap Z$. Then $\bar{H}$ and $\bar{K}$ induce the same permutation representation, $\ker_{\bar{G}}\bar{H}=1$, and $F^*(\bar{G})\cong Z_q\times PSL_n(r)$ or a central quotient of $SL_n(r)$. If $[G:H]=pq$, the former must occur by Proposition 5.1.

EXAMPLE 4. Let P and Q be two p-groups of exponent p of the same order. Such groups occur in [18]. The regular representation for P or Q for elements of order p has $|P|/p$ p-cycles. Considering each as a subgroup of $S_{|P|}$, the permutation characters are the same. They certainly need not be isomorphic.

4. SUBGROUPS OF INDEX p^a

In this section we collect some results about subgroups H and K of index p^a in G. Again let V be the module affording I_H^G and W the module affording I_K^G. We have seen in Section 2 that V and W being isomorphic as R modules where R is $\mathbb{Z}_p$ or a field of characteristic p is equivalent to H and K having conjugate Sylow p-subgroups. Two permutation modules isomorphic over the p-adic integers are isomorphic over $\mathbb{Q}_p$ and so are isomorphic viewed over $\mathbb{C}$. This means they have the same character. However, two permutation modules with the same character need not be isomorphic over $\mathbb{Z}_p$. The following result gives a condition to guarantee such representations are isomorphic over $\mathbb{Z}_p$.

THEOREM 4.1. *Suppose H and K are subgroups of index p^a in G for which I_H^G and I_K^G are isomorphic over $\mathbb{C}$. Suppose Q is a Sylow p-subgroup of H, P is a Sylow p-subgroup of G, and $Q \lhd A \lhd P$ with A/Q cyclic. Then I_H^G and I_K^G are isomorphic over R where R is $\mathbb{Z}_p$ or a field of characteristic p.*

Proof. As $HP = G$, Lemma 2.2(ii) gives $I_{P\cap H}^P \cong I_{P\cap K}^P$ as modules over $\mathbb{C}$. As Q is a Sylow p-subgroup of H contained in P, $P\cap H = Q$. Assume the kernels of each permutation representation are trivial by factoring them out if necessary. Let φ be the character of I_Q^P. Since $Q \lhd A \lhd P$, $\varphi(x) = 0$ if $x \in P - A$ as conjugates of such x are in $P - A$ also and so not in Q. If $y \in P \cap K$; $\varphi(y) \neq 0$ and so $y \in A$. In particular $P \cap K \subseteq A$. Let $P \cap K = S$. Now

$$\varphi_A = \sum_{g \in T} 1_{Q^g}^A = \sum_{g\in T} 1_{S^g}^A$$

where T is a transversal for A in P. As $Q \lhd A \lhd P$, the groups Q^g are the kernels of the linear characters whose values are $|A:Q|$ roots of 1. The multiplicity of a given Q^g is the multiplicity of a fixed such character in φ_A. As A/Q^q is abelian and $\bigcap_{g\in T} Q^g$ is trivial because we are assuming 1_H^G is faithful, A is abelian. Now Q^g is a normal subgroup of A of index $|A:Q|$. There are $|T|$ such subgroups. The linear characters which are constituents of $1_{S^g}^A$ all have S^g in their kernel. A constituent of 1_Q^A whose value is an $|A:Q|$ root of 1 must occur as a constituent of $1_{S^g}^A$ for some g. Restricting to S^g of index $|A:Q|$ gives the trivial character and so $S^g = Q$. In particular a Sylow p-subgroup of K is conjugate to a Sylow p-subgroup of H and so I_H^G and I_K^G are isomorphic over R by Corollary 2.7.

COROLLARY 4.2. *If H and K are of index p^a in G with $a \leqslant 2$ and $I_H^G \cong I_K^G$ over $\mathbb{C}$, then $I_H^G \cong I_K^G$ over $\mathbb{Z}_p$ or a field of characteristic p.*

Proof. As $|P:Q| = p$ or p^2, an A as in Theorem 4.1 can be found.

Remark. If $p \neq 11$ or $p \neq (q^n - 1)/(q-1)$, $n \geqslant 3$, the conditions of Corollary 4.2 imply H and K are conjugate by [13, Corollary 3.3].

Let Π be a set of primes and let $\Gamma(\Pi)$ be the set of simple groups with more than one conjugate class of Π-complements. If Π is a single prime p, the result of [13] shows

$$\Gamma(p) = \{PSL_n(q);\, p^t = (q^n - 1)/(q-1), n \geqslant 3\}$$

unless $p = 11$ in which case $L_2(11)$ is also in $\Gamma(p)$. One can show $\Gamma(p)$ is always finite. It is a number theoretic problem to determine when $\Gamma(p)$ is empty. It has been shown by Arad and Ward [1] and the first author [13] that $\Gamma(2)$ is empty. M. Ward has conjectured that $\Gamma(\Pi)$ is empty whenever 2 is in Π. As well as for $\Gamma(2)$, it is known that $\Gamma(p)$ is empty for p a Fermat prime and when $p - 1 = 2^\alpha 3^\beta$ with $p \neq (q^3 - 1)/(q-1)$. We conjecture that $\{p \mid \Gamma(p) \text{ is nonempty}\}$ has density 0.

If G is a group in $\Gamma(p)$, G has two conjugate classes of subgroups of index p^a by definition. They are both maximal. The properties of maximal subgroups of index p^a are more stringent than those of arbitrary subgroups of index p^a. Of course, such a subgroup is contained in a maximal subgroup of index p^b with $b \leqslant a$. The next result builds on Section 5 of [13].

THEOREM 4.3. *Let H be a maximal subgroup of index p^a in G. Set $L = \ker_G(H)$. If no factor of a composition series for G/L is in $\Gamma(p)$, then $I_H^G \cong I_K^G$ over $\mathbb{Z}_p$ or a field of characteristic p implies H and K are conjugate.*

Proof. Assume $L = 1$ and so H and K contain no normal subgroups. Here K is also maximal as in [13, Sect. 5]. By [13, 5.2], $G = AH = AK$ where $A = F^*(G)$ is an elementary abelian p-group which is minimal normal and $A \cap H = A \cap K = 1$. The possibility in [13, 5.2(b)] is ruled out by the hypothesis. By conjugating we can assume H and K have a common Sylow p-subgroup Q by Corollary 2.2. Now as in [13, Example 4.3] H and K correspond to elements α and β in $H^1(G/A, A)$. Since the restriction map

$$H^1(G/A, A) \to H^1(QA/A, A)$$

is injective it follows that $\alpha = \beta$ and so H and K are conjugate in G.

We showed in Example 3a that $GL_2(3)$ has two nonconjugate subgroups of index 8 with $I_H^G \cong I_K^G$ over $\mathbb{Z}_2$ and over $GF(2)$. The composition factors of $GL_2(3)$ are of orders 2 and 3 and are not in $\Gamma(2)$. As was mentioned above $\Gamma(2)$ is empty. This shows that the condition on maximality in Theorem 4.3 is necessary. We do not know of similar examples for odd p.

We complete this section with a result about conjugacy of Π-complements. This extends [13, 3.2] where it was assumed $\Pi = \{p\}$ and $\Gamma(p)$ was empty.

THEOREM 4.4. *Let G be a finite group with Π-complements H and K. If no composition factor of G is in $\Gamma(\Pi)$, H and K must be conjugate.*

Proof. Use induction on $|G|$ and choose a minimal normal subgroup A of G. If A is a Π'-group, then $A \leqslant H \cap K$ and the result follows by induction on G/A. If A is a Π-group, then AH and AK are conjugate by induction and H and K are conjugate by the Schur–Zassenhaus Theorem. This leaves $A \cong S \times S \times \cdots \times S$ where S is a nonabelian simple group with prime divisors in Π and Π'. Since $S \notin \Gamma(\Pi)$, $L = H \cap A$ and $K \cap A$ are conjugate in A. By conjugating assume $L = K \cap A$. Since

$$\{L^G\} = \{L^A\}, \qquad G = AN_G(L).$$

Set $N = N_G(L)$. Thus $N \supseteq \langle H, K \rangle$. Since $(A \cap N)/L$ is a Π-group, L is a Π'-group, and $N/N \cap A \cong G/A$, N satisfies the hypothesis of the theorem and so H and K are conjugate in N by induction.

5. PRIMITIVE GROUPS OF SQUAREFREE DEGREE

In this section, maximal subgroups of squarefree index are investigated. Proposition 5.2 reduces this to a problem about simple groups. In particular, we determine all possibilities for maximal subgroups of index pq in a simple group.

Recall that a group L is called quasisimple if $L = L'$ and $L/Z(L)$ is simple. If L is also subnormal in G, then L is called a component of G. Then $E(G)$ is the subgroup of G generated by all components. Moreover, $E(G)$ is a central product of all the components of G. The generalized Fitting subgroup of G is $F^*(G) = E(G)\,F(G)$, where $F(G)$ is the Fitting subgroup of G. We will need the important fact that $F^*(G)$ contains its own centralizer.

PROPOSITION 5.1. *Suppose $[G:H] = n$ is squarefree. Set $E = E(G)$ and let L be a component of G. Then*

(1) $Z(E) \leqslant H$.

(2) *Either* $H \geqslant L$ *or* $H \leqslant N_G(L)$.

(3) *If* $Q = \langle L^H \rangle = \langle L^G \rangle$, *either* $Q \leqslant H$ *or* $Q = L$.

Proof. Set $M = H \cap E$. Since $E \lhd G$, $[E:M]$ is squarefree also. Let $Z = Z(E)$, and consider the transfer homomorphism σ from E to MZ/M. If p is a prime divisor of $[MZ:M]$, then $(p, e) = 1$, where $e = [E:MZ]$. If $z \in Z$, then $\sigma(z) = z^e M$. Hence $\sigma(Z) = MZ/M$ and $E = Z(\ker \sigma)$. Since E is perfect, $E = \ker \sigma$ and $Z \leqslant M \leqslant H$.

Suppose (2) fails. By (1), we can pass to $G/Z(E)$ and so assume $Z(E) = 1$. Now there exists a component L_1 of G not contained in or normalized by H. So for some $h \in H$, $L_2 = L_1^h \neq L_1$. Since $Z(E) = 1$, $E = L_1 \times L_2 \times \cdots \times L_r$, where L_i are the components of G. Let σ_i denote the projection of E onto L_i. Since $H \cap L \neq L_i$ and $H \cap L_i \lhd (H \cap E)$ for $i = 1$ and 2, $\sigma_i(H \cap E) \neq L_i$ for $i = 1$ and 2. Moreover, $H \cap E \leqslant \sigma_1(H \cap E)\,\sigma_2(H \cap E)\,L_3 \cdots L_r$, and so $[E:H \cap E]$ is a multiple of $[L_1:\sigma_1(H \cap E)][L_2:\sigma_2(H \cap E] = [L_1:\sigma_1(H \cap E)]^2$ and is not squarefree. Thus (2) holds.

Now (3) follows easily, for if $L \leqslant H$, then $Q \leqslant H$, while if L is not contained in H, then by (2), $Q = L$.

PROPOSITION 5.2. *Let* G *be a faithful primitive permutation group on* Ω *with* $|\Omega| = n$ *squarefree. Then* $F^*(G)$ *is simple and acts transitively on* Ω.

Proof. If $F(G) \neq 1$, then n is prime, $|F(G)| = n$, and the result is clear. So assume $F(G) = 1$. Thus G has a component L. Set $Q = \langle L^G \rangle$ and let H be the stabilizer of a point. Since $G = QH$, $Q = \langle L^H \rangle$ and by Proposition 5.1, $L \lhd G$ and $G = LH$. If M were any other component, then $[M:H \cap M]$ is squarefree and so $1 \neq H \cap M \leqslant C_H(L) \lhd G$. Since H contains no normal subgroups, this cannot occur. Similarly, $Z(L) \leqslant H$ by Proposition 5.1 and so $Z(L) = 1$. Thus L is simple and $G = HL$ as desired.

We now consider the simple groups. Subgroups of squarefree index are quite rare. The case of prime index is well known (cf. [10]), since by Burnside's Theorem, the action is doubly transitive.

PROPOSITION 5.3. *Let* $G = \mathrm{Alt}(\Omega)$ *with* $|\Omega| = m > 8$. *If* $[G:H] = n$ *is squarefree, then either*

(a) H *is intransitive, or*

(b) $m = 2k$, $\Omega = \Omega_1 \cup \Omega_2$ *with* $|\Omega_i| = k$ *and* H *acts on* $\{\Omega_1, \Omega_2\}$.

If $n = pq$, (b) *does not occur,* H *has an orbit* Δ *of size at most* 2, *and* H *is the stabilizer of* Δ.

Proof. Assume H is transitive. If H does not act primitively, there is a partition $\{\Omega_1,\ldots,\Omega_s\}$ of Ω with $|\Omega_i| = k = m/s$ such that H permutes the Ω_i. If $s=2$, then (b) holds. So assume $2 < s < m$. Let $\tilde{H}$ be the subgroup of G which permutes the Ω_i. Then

$$[G:\tilde{H}] = \frac{m!}{(k!)^s s!} \qquad \text{is squarefree.}$$

If $s, k \geqslant 4$, choose a prime p such that $l = \max\{s, k\} < p < 2l \leqslant m/2$ (this is possible by Bertrand's Postulate). Then $p^2 \mid [G:\tilde{H}]$, a contradiction. If $k=2$, then $9 \mid [G:\tilde{H}]$ (as $s \geqslant 5$). If $k=3$, $4 \mid [G:\tilde{H}]$ for $s=3$ and $25 \mid [G:\tilde{H}]$ for $s \geqslant 4$. So the only possibility is that $s=3$ and $k \geqslant 4$. It can be shown for $k \neq 7$ using the Prime Number Theorem that there is a prime p with $k < p \leqslant 3k/2$. Then $p^2 \mid [G:\tilde{H}]$. For $k=7$, 2^2 or $3^2 \mid [G:\tilde{H}]$.

So assume H acts primitively. Let $T \in \mathrm{Syl}_5(G)$ with $T \cap H \in \mathrm{Syl}_5(H)$. Since $[T:T\cap H] = 1$ or 5, it follows that H contains a five cycle or a product of two disjoint five cycles. By [1, Theorems 13.9 and 13.10], this implies $H = G$ for $n \geqslant 13$. For $9 \leqslant n \leqslant 12$, $H = G$ by inspection.

If $n = pq$, then $n < m^2$. In case (b), $n \geqslant (2k)!/2(k!)^2 \geqslant m^2$ as $m \geqslant 9$. So (a) holds and H has an orbit Δ with $t = |\Delta| \leqslant m/2$. Let $\tilde{H}$ be the stabilizer of Δ. Then $[G:\tilde{H}] = m!|t!(m-t)! < m^2$. This implies $t \leqslant 2$ as $m \geqslant 9$. If $t=2$, then $[G:\tilde{H}] = m(m-1)/2$ is not prime and so $H = \tilde{H}$. If $t=1$, then $[G:\tilde{H}] = m$. If $m = pq$, then $H = \tilde{H}$. Otherwise say $m = p$ and $\tilde{H} \cong A_{m-1}$ has a subgroup of index $q < m$. However, as $m-1$ is even, $q < m-1$ and this contradiction yields the result.

Note that (b) can actually occur (e.g., take $m = 12$). However, it is likely that this occurs only finitely many times.

A beautiful result of Seitz [20] will handle almost all of the Chevalley groups. Let G be a simple Chevalley Group defined over $GF(r)$, $r = l^a$, l prime. Let Σ be a root system for G and set $U = \langle U_r \mid r \in \Sigma^+ \rangle$. The next result is well known (cf. [7]).

LEMMA 5.4. *If $G \neq A_1(r)$, then $Z(U) \leqslant \Phi(U)$, the Frattini subgroup of U. Moreover, if α is the highest weight of Σ, then $Z(U_\alpha) \leqslant Z(U)$.*

PROPOSITION 5.5. *If $G \neq A_1(r)$ and H is a subgroup with $r^2 \nmid [G:H]$, then $H \leqslant P$, a parabolic subgroup of G.*

Proof. Let $\Gamma(H) = \{J^g < H \mid g \in G\}$ where $J = Z(U_\alpha)$, α the highest weight. Also by the lemma, if $V \in \mathrm{Syl}_l(H)$ and $V \leqslant S \in \mathrm{Syl}_l(G)$, then $V \geqslant C_S(V)$. Hence V is full (as defined in [20]). Thus by [20, Theorem 4] if l is odd and $r > 3$, H is contained in a parabolic subgroup of G. If $l = 2$ and $r > 3$, then either H is contained in a parabolic subgroup of G or

$H \leqslant N_G(Y)$ for a quasisimple subgroup Y generated by long root subgroups of G and Y is a Chevalley group over $GF(r)$. An inspection of the orders of Aut Y precludes the possibility that $l^2 \nmid [G:H]$.

Unfortunately, we still must deal with the case $r=2$ or 3. However, by the above we can assume G has rank $\geqslant 2$ and is not of type ${}^2F_4$. Moreover, by the Borel–Tits Theorem if H is not contained in a parabolic subgroup, then $O_l(H)=1$. By Cooperstein [4], $X=\langle \Gamma(H) \rangle = X_1 \cdots X_m$, where $X_i = \langle \Gamma_i \rangle$, $[X_i, X_j]=1$ if $i \neq j$, $\Gamma(H)$ is a disjoint union of the Γ_i, and Γ_i is a single conjugacy class in X_i. Since $O_l(H)=1$, $O_l(X_i)=1$ for each i. By conjugating we can assume $J \subseteq X_1 \cap Z(V)$. Thus for any $v \in V$, $J = J^v \subseteq X_1 \cap X_1^v \subseteq Z(X_1) \cap O_l(X_1)$ unless $X_1 = X_1^v$. Hence $V \leqslant N_G(X_1) = N$.

We claim N is not contained in a parabolic subgroup P of G. If so, set $Q = O_l(P)$. Now $QV = V$ or QV is a Sylow $-l$ subgroup of G. In either case, by the lemma, there exists $K \leqslant Z(QV)$ with $K \in \Gamma(G)$. Moreover, by the lemma, $K \leqslant V$ and so $K \leqslant C_l(Q) \cap X \leqslant Q \cap X \leqslant O_l(X) = 1$. This proves the claim. Now the result follows by examining the list of subgroups Y generated by conjugates of J in Kantor [16] and Cooperstein [5, 6] and determining that either $M = N_G(Y)$ is contained in a parabolic subgroup or $l^2 \mid [G:M]$.

We can now list all maximal subgroups of index pq in a simple group (Table I). For $G = L_2(r)$ or A_n, $n<9$, all subgroups are known. If G is a Chevalley group, one can just check which parabolic subgroups can possibly have index pq (using some elementary number theory). If $G = {}^2F_4(2)'$ or a sporadic group other than listed in the table, it follows from the character tables that there are no subgroups of index pq. For the sporadic groups listed, all maximal subgroups are known.

We conclude this section with a determination of all primitive groups of degree pq. Note in Proposition 5.2 that one only concludes that $F^*(G)$ acts transitively not primitively. However, for $n = pq$, this is true except for the one case 5.6(b) below.

PROPOSITION 5.6. *Let G be a faithful primitive group on Ω with $|\Omega| = pq$ (p, q distinct primes). Then $F^*(G)$ is a nonabelian simple group and either*

(a) *$F^*(G)$ acts primitively on Ω (and so is given in Table I), or*

(b) *$G = PGL_2(11)$ is acting on the cosets of $N_G(T)$ for $T \in \mathrm{Syl}_2(G')$ and $pq = 55$.*

Proof. Let H be the stabilizer of a point. By Proposition 5.2, $L = F^*(G)$ is a nonabelian simple group. If $H \cap L$ is maximal in L, then (a) holds. Otherwise $H \cap L < M < L$ with $[L:M] = p$. Thus by [13], $L = PSL_n(r)$ or $PSL_2(11)$, where in the first case M is the stabilizer of a line or hyperplane and in the second case $M \cong A_5$. In the first case $H \cap L \lhd M$ and so H is

TABLE I

G	$n=pq$	Rank	Orbit lengths	H	Notes
$L_2(19)$	57	4		$L_2(5)$	Two classes same character
$L_2(29)$	$7\cdot 29$	$\geqslant 8$			
$L_2(59)$	$29\cdot 59$	$\geqslant 30$			
$L_2(61)$	$31\cdot 63$	$\geqslant 32$			
$L_2(r)$ $(r\geqslant 13)$	$\frac{r(r+1)}{2}$	$\geqslant\frac{r+1}{2}$		D_m, $m=\frac{r-1}{2}$	
$L_2(r)$ $(r\geqslant 11)$	$\frac{r(r-1)}{2}$	$\geqslant\frac{r+1}{2}$		D_m, $m=\frac{r+1}{2}$	
A_7	35	4	1, 4, 12, 18	$(A_3\times A_4)2$	
A_5	6	2	1, 5	D_5	
A_5	10	3	1, 3, 6	S_3	
A_6	6	2	1, 5	A_5	(Intransitive on 6 points)
A_6	6	2	1, 5	A_5	(Transitive on 6 points)
A_6	10	2	1, 9	$N(T)$	$T\in\mathrm{Syl}_3(A_6)$
A_6	15	3	1, 6, 8	S_4	(Transitive)
A_6	15	3	1, 6, 8	S_4	(Intransitive)
A_7	15	2	1, 14	$L_3(2)$	
A_7	21	3	1, 10, 10	S_5	
A_l $(l\geqslant 10)$	l	2	$1, l-1$	A_{l-1}	
A_l $(l\geqslant 11)$	$\frac{l(l-1)}{2}$	3	$1, 2(l-2), \frac{(l-2)(l-3)}{2}$	S_{l-2}	
M_{11}	55	3	1, 10, 44	3^2QD_{16}	
M_{22}	22	2	1, 21	M_{21}	
M_{22}	77	3	1, 21, 55	2^4A_6	
M_{23}	253	3	1, 42, 210	$M_{21}2$	Same character $1+22+230$
M_{23}	253	3	1, 112, 140	2^4A_7	
$L_l(r)$ $(r=s^a$, l prime, $a=l^t)$	$\frac{r^l-1}{r-1}$	2	$1, n-1$	Stabilizer of a projective point or hyperplane (Two classes with same character if $l\geqslant 3$)	
$U_3(r^2)$	r^3+1 ($n=r^3+1=(r+1)(r^2-r+1)$ $r+1$ must be a Fermat prime, r^2-r+1 also a prime (e.g., $r=4$, 16))	2	$1, n-1$	Stabilizer of a singular line	r even
$Sz(2^{2m+1})$	$4^{2m+1}+1$ $n=4^{2m+1}+1$ must be a product of two primes (e.g., $m=1$, $n=65$)	2	$1, n-1$	Borel subgroup	
$Sp_4(r)$	$\frac{r^4-1}{r-1}$ $n=(r+1)(r^2+1)$ a product of two consecutive Fermat primes, e.g., $r=4$, $n=5\cdot 17=85$ $r=16$, $n=17\cdot 257=4369$	3	$1, r^2+r, r^3$	Either of the maximal parabolics	r even Different characters

properly contained in $N_G(H \cap L)$, a contradiction. So necessarily, $L = PSL_2(11)$, $G = PGL_2(11)$, $A_4 \cong H \cap L = N_L(T)$, $T \in \mathrm{Syl}_2(L)$. Thus $H = N_G(T)$ and (b) holds.

6. Subgroups of Index pq

In this section, we determine the structure of permutation groups of degree pq. The primitive ones were described in the previous setion. We also determine when there can be nonconjugate subgroups of index pq inducing the same permutation representation. The first case is when $E(G) = 1$. Note this result does not depend on the classification theorem for simple groups.

Theorem 6.1. *Let H and K be subgroups of index pq in G (p, q distinct primes) such that*

(i) $1_H^G \cong 1_K^G$, *and*

(ii) $E(G/L) = 1$, *where* $L = \ker_G H = \bigcap H^g$.

Then H and K are conjugate in G. In particular, this holds when G/L is solvable.

Proof. Since $L = \ker_G K$ by (i), we can assume $L = 1$. Thus $F = F(G) = O_p(G) \times O_q(G)$. If $pq \mid |F|$, then $G = HF$ and so $H \cap F \lhd G$. Thus $H \cap F = 1$ and F is cyclic. Since $C_G(F) = F$, H embeds in $\mathrm{Aut}\, F$. Hence either H is cyclic or $H = N_G(R)$ for some $R \in \mathrm{Syl}_r(G)$ with $r \mid (p-1, q-1)$. In the first case, (i) implies that H and K are conjugate. In the second case, the result is obvious.

So assume $F^*(G) = O_p(G) = A$. If $|A| = p$, then as $A \geqslant C_G(A)$, $G/A \cong H$ is cyclic and H and K are conjugate. So $|A| > p$ and $A \cap H \neq 1$. Set $M = HA$. Since

$$1_H^G|_A = \Sigma 1_{A \cap H^x}^A = \Sigma 1_{A \cap K^y}^A,$$

by conjugating we can assume $A \cap H = A \cap K = B$ (since the kernel of any nontrivial constituent of $1_{A \cap H}^A$ is $A \cap H$). Hence $\langle H, K \rangle \leqslant N_G(B) \neq G$. Thus $N_G(B) = M$ has index q in G. Note $BH = HB = H$. If $x \in G - M$, then $x^{-1}BxB = A$, and so $HxH = Hxx^{-1}BxBH = HxAH = MxM$. Similarly, $KxH = MxM$ for $x \notin M$. Since the number of (H, K) double cosets in G is $(1_H^G, 1_K^G) = (1_H^G, 1_H^G)$ is the number of (H, H) double cosets in G, it follows that $M \neq KH$. Set $S = \ker_M H$. Since $KS \subseteq KH \neq M$, $S \leqslant K$. Since $p = [M:H]$, $p \nmid [H:S]$. Thus H/S and K/S are complements to the normal Sylow p-subgroup AS/S in M/S. Thus H and K are conjugate in M.

One may ask whether Theorem 6.1 holds for squarefree index when G is solvable. We are now ready for the main result of this section.

THEOREM 6.2. *Let H be a subgroup of G of index pq, where p and q are distinct primes and* $\ker_G H = 1$. *Let $\Gamma = \{K < G \mid I_K^G = I_H^G\}$. One of the following holds (up to interchanging p and q):*

(1) *$E(G) = 1$ and $\Gamma = H^G$.*

(2) *$F^*(G) = L_1 \times \cdots \times L_q$, where the L_i are the conjugates of the simple component L_1 and $H_1 = H \cap L_1$ has index p in L_1. Moreover, $H \cap F^*(G) = H_1 \times L_2 \times \cdots \times L_q$ and $H = N_G(H \cap F^*(G))$. Thus Γ consists of a unique class if $L_i \notin \Gamma(p)$; two classes if $L_i \in \Gamma(p)$.*

(3) *$F^*(G) = L_1 \times L_2$, where L_1 and L_2 are simple normal components of G, $H \cap F^*(G) = H_1 \times H_2$, where $H_i = H \cap L_i$, $[L_1 : H_1] = p$, and $[L_2 : H_2] = q$. Moreover, $H = N_G(H_1 \times H_2)$, and so Γ consists of one, two, or four classes depending upon whether $L_1 \in \Gamma(p)$ and/or $L_2 \in \Gamma(q)$.*

(4) *$F^*(G) = L$ is simple, $[L : H \cap L] = pq$, and $H \cap L$ is maximal in L. Then $H = N_G(H \cap L)$, L is given in Table I, and Γ consists of one or two classes as given in Table I.*

(5) *$F^*(G) = L \cong L_2(11)$, $[L : H \cap L] = 55$, and $H = N_G(T)$ for some $T \in \mathrm{Syl}_2(L)$. Then $\Gamma = H^G$, and $H = N_G(H \cap L)$.*

(6) *$F^*(G) = L \cong L_n(r)$, where $p = (r^n - 1)/(r - 1)$, $q \mid (r - 1)$, $[L : H \cap L] = pq$, and $M = N_L(H \cap L)$ has index p in L. Then $K \in \Gamma$ is conjugate to H if and only if $H \cap L$ and $K \cap L$ are conjugate in L. Hence Γ consists of one or two classes depending upon whether $n = 2$ or $n > 2$ (and so $L \in \Gamma(p)$).*

(7) *$F^*(G) = L \times Z_q$, where $L \cong L_n(r)$, $p = (r^n - 1)/(r - 1)$, $q \mid (r - 1)$, $[L : H \cap L] = pq$, and $M = N_L(H \cap L)$ has index p in L. In this case, Γ will consist of two classes. (See Example 3. Note if $n > 2$, $L \in \Gamma(p)$, while if $n = 2$, p is a Fermat prime and $p \equiv 2 \bmod q$.)*

(8) *$F^*(G) = L$ or $L \times Z_q$, where L is simple and $[L : H \cap L] = p$. Then $K \in \Gamma$ is conjugate to H if and only if $H \cap L$ and $K \cap L$ are conjugate in G. Thus $\Gamma = H^G$ or Γ consists of two classes if both $L \in \Gamma(p)$ and $G = LN_G(H \cap L)$.*

Note in all cases $K \in \Gamma$ is conjugate to H if and only if $H \cap E(G)$ and $K \cap E(G)$ are conjugate in G. Moreover Γ consists of at most two classes unless (3) applies, in which case there are one, two, or four classes.

Proof. If $E = E(G) = 1$, then (1) holds by Theorem 6.1. So assume $E \neq 1$. By Proposition 5.1, $Z(E) = 1$, and so all components of G are simple.

First assume G has a nonnormal component L_1. By conjugating, we can take $H_1 = H \cap L_1 \neq L_1$. By Proposition 5.1, $H \leqslant N_G(L_1)$ and so $G \neq HL_1$. Thus $[L_1 : H_1] = p$. Note that $HL_1 \leqslant N_G(L_1) \neq G$, and so $[G : N_G(L_1)] = q$. Thus L_1 has exactly q conjugates in G. Moreover, $H \leqslant N_G(H_1) \leqslant N_G(L_1)$, and so $H = N_G(H_1) = N_G(E \cap H)$. Now (2) follows.

We can now assume all components of G are normal. Let $E = L_1 \times \cdots \times L_r$. Let σ_i denote the projection of E onto L_i. Since H does not contain L_i and $\sigma_i(E \cap H)$ normalizes $H_i = H \cap L_i$, $\sigma_i(E \cap H) \neq L_i$. Thus $[E : E \cap H]$ divides $[L_1 : \sigma_1(E \cap H)] \cdots [L_r : \sigma_r(E \cap H)]$, and $r \leqslant 2$. Moreover, if $r = 2$, $\sigma_i(E \cap H) = H_i$, $E \cap H = H_1 \times H_2$, $[L_1 : H_1] = p$, and $[L_2 : H_2] = q$. Thus $G = HE = NE$, where $N = N_G(E \cap H)$. Since $N \cap E = H \cap E$, $H = N \geqslant F(G)$. Thus (3) holds.

Now assume $E = L$ is simple. First consider the case where $[L : H \cap L] = pq$, and so $G = HL$ and $N = N_G(H \cap L) = HN_L(H \cap L)$. If $H \cap L$ is maximal in L, $H = N \geqslant F(G)$ and (4) holds. If $H \cap L$ is not maximal in L but $N_L(H \cap L) = H \cap L$, $H = N \geqslant F(G)$ and by [13], (5) holds. If $M = N_L(H \cap L)$ properly contains $H \cap L$, then again by [13], $L = L_n(r)$, where $(r^n - 1)/(r - 1) = p = [L : M]$, $q \mid (r - 1)$, and M is the stabilizer of a line or hyperplane. Set $F = F(G)$. Note $H \cap F = 1$, as $H \cap F \lhd HE = G$. Also $HF \leqslant N$ and so $|F| = 1$ or q. Since $C_G(F^*(G)) = F$ and $G = HE$, it follows that $G/F^*(G)$ embeds in $P\Gamma L_n(r)/L_n(r) \times Z_{q-1}$ and $q \nmid [G : F^*(G)]$. Thus $M/H \cap L$ is a normal Sylow q-subgroup of $N/H \cap L$ and $H/H \cap L$ is a complement. Hence, if $K \in \Gamma$ and $H \cap L$ and $K \cap L$ are conjugate, it follows that H and K are conjugate and so (6) or (7) holds.

Finally, consider the case $[L : H \cap L] = p$. Let $F = F(G)$. Then $H \cap F^*(G) = (H \cap L) \times (H \cap F)$. So if $F \neq 1$, $G = HF^*(G) = N_G(H \cap F)$. Thus $H \cap F = 1$ and so $|F| = q$. If $H = N_G(H \cap L) = N$, then $K = N_G(K \cap L)$ for any $K \in \Gamma$, and so (8) holds. In this case $G \neq LN_G(H \cap L)$, Γ consists of one class, and $F^*(G) = L$. If $H \neq N$, then $H = N \cap HL$. If $K \in \Gamma$, then $I^G_{HL} \cong I^G_{KL}$ by Lemma 2.10. Since $G/\ker_G HL$ is solvable, this implies HL and KL are conjugate. So assume $HL = KL$. Note if $H \cap L$ and $K \cap L$ are conjugate in G, they are conjugate in L (for $H \neq N$ implies $G = NL$), and so we can also assume $H \cap L = K \cap L$. Then $H = HL \cap N = KL \cap N = K$ and so (8) holds. Here $G = LN$ and so Γ consists of two classes if and only if L is in $\Gamma(p)$.

Theorem B follows.

References

1. F. Arad and M. Ward, New criteria for the solvability of finite groups, *J. Algebra* **77** (1982), 234–246.
2. R. Brauer and C. Nesbitt, On the modular characters of groups, *Ann. of Math. (2)* **42** (1942), 556–590.

3. D. BURRY, Scott modules and lower defect groups, *Comm. Algebra* **10** (1982), 1855–1872.
4. B. COOPERSTEIN, Minimal degree for a permutation representation of a classical group, *Israel J. Math.* **30** (1978), 213–235.
5. B. COOPERSTEIN, The geometry of root subgroups in exceptional groups, I, *Geom. Dedicata* **8** (1979), 317–381.
6. B. COOPERSTEIN, The geometry of root subgroups in exceptional groups, II, preprint.
7. C. CURTIS, W. KANTOR, AND G. SEITZ, The 2-transitive permutation representations of the finite Chevalley groups, *Trans. Amer. Math. Soc.* **218** (1976), 1–59.
8. C. CURTIS AND I. REINER, "Methods of Representation Theory—With Applications to Finite Groups and Orders," Vol. I, Wiley, New York, 1981.
9. L. DORNHOFF, "Group Representation Theory," Vols. I, II, Dekker, New York, 1971–1972.
10. W. FEIT, Some consequences of the classification of finite simple groups, *in* "Proceedings, Symposia in Pure Mathematics," Vol. 37, Amer. Math. Soc., Providence, R.I., 1980.
11. W. FEIT, "The Representation Theory of Finite Groups," North-Holland, Amsterdam/New York/Oxford, 1982.
12. J. GREEN, Multiplicities, Scott modules, and lower defect groups, *J. London Math. Soc.* **28** (1983), 282–292.
13. R. GURALNICK, Subgroups inducing the same permutation representation, *J. Algebra* **81** (1983), 312–319.
14. G. HIGMAN, On the simple group of D. G. Higman and C. C. Sims, *Illinois J. Math.* **13** (1969), 74–80.
15. I. M. ISAACS, Fixed points and Π-complements in Π-separable groups, *Arch. Math.* **39** (1982), 5–8.
16. W. KANTOR, Subgroups of classical groups generated by elements central in a long root subgroup, *Trans. Amer. Math. Soc.* **248** (1979), 347–379.
17. J. MARANDA, On p-adic integral representations of finite groups, *Canad. J. Math.* **5** (1953), 344–355.
18. R. PERLIS, On the equation $\zeta_K(s) = \zeta_{K'}(s)$, *J. Number Theory* **9** (1977), 342–360.
19. R. PERLIS, On the class numbers of arithmetically equivalent fields, *J. Number Theory* **10** (1978), 489–509.
20. G. SEITZ, Unipotent subgroups of groups of Lie type, *J. Algebra* **84** (1983), 253–278.
21. H. WIELANDT, "Finite Permutation Groups," Academic Press, New York, 1964.
22. L. SCOTT, Modular permutation representations, *Trans. Amer. Math. Soc.* **175** (1973), 101–121.